Sommaire

1 **Techniques et outils des hackers et des administrateurs réseaux** **27**

1.1 Techniques **30**
Exemple 30
1.2 Crééz votre environemment de test **31**
Virtual Machine 31
1.3 Quelques types de scanners **53**
Les scanners de ports 54
Scanner de failles système 64
Scanner de serveur avec des failles système Unicode URLSCANNER 72
Scanner de vulnérabilités Web Acunetix 76
Tester des vulnérabilités des pages http et HTTPS avec N-Stealth HTTP Security Scanner 80
Scanner de Proxy ProxyHunter 85
Scanners de boîtes vocales 91

2 **Repérage et interceptions des adresses IP et des domaines sur Internet** **93**

2.1 WHOIS **95**
Whois : les serveurs dans les différents continents 95

Uwhois 98
2.2 **Le Whois magique 100**
2.3 **Les traceurs 102**
Programme de traçage VisualRoute 102
Programme de traçage Neo Trace 107
Trouver un pirate grâce au traçage MS DOS de Windows 108
2.4 **Les sniffers et renifleurs 109**
Logiciel de sniffer Ettercap 111
Logiciel de sniffer Ethereal et les exploits de spoofing 117
Reniflage avec Netstat 131
Logiciel de sniffer X-NetStat Professional 134
Recherche des informations sur les systèmes d'exploitation 143
2.5 **Les sniffers de réseaux sans fil 145**
Sniffer wireless Cain & Abel 146
Sniffer Wireless Net stumble 147
Sniffer Wireless moniteur Airo Peek 148

3 Protéger sa vie privée 151

3.1 **Mail anonyme 153**
Envoi d'un email avec l'Invite de commandes 155
3.2 **Protéger sa machine contre les connexions Telnet 159**
3.3 **Se protéger contre les caches 159**
3.4 **Retirer l'enregistrement automatique des mots de passe d'Internet Explorer 161**
Création d'un compte 162
3.5 **Logiciels antimouchards 164**
Ad-Aware, un antimouchard puissant 164
Anti-ad-aware 167
Spybot-search & destroy, l'ennemi numéro 1 des mouchards 168
Cookie Pal 1.7 démo, la terreur des mouchards 169
XP-Antispy, l'antimouchard Microsoft 170
Se débarrasser manuellement des espions d'ICQ 172
Désactiver l'espion de Media Player 173
Effacer les mouchards d'ActiveX 174
3.6 **Popups sur le Web 175**
Le roi des Eliminer les pop ups et spywares, Stopzilla 175
Avantages de Stopzilla 176
3.7 **Lutter contre le harcèlement du spamming 176**
Comment font-ils pour atteindre votre boite email ? 177
Qui sont les spammeurs ? 177
Déni de service en Spamassasin 3 179
Intérêt de trouver les spammeurs 180
Les spammeurs de boîtes aux lettres 182
Retrouver les spammeurs avec Spam Buster 183
3.8 **Filtres de Spams 183**

4 Types de connexion sur le réseau 185

4.1 Connexion à Internet avec un camouflage 187
Steganos Internet anonyme 192
Anonyme Stealther 195
4.2 Usurpation d'adresse IP 202
Décryptage des mots de passe par connexion VPN 203
Connexion VPN 205
Établir une connexion VPN 206
Protocoles VPN 207
Illustration 208
4.3 La connexion à distance 208
Configurer une connexion distance 208
Illustration 210
4.4 Administrateur à distance Logiciel Netbus 2.20 211
4.5 Connexion via Telnet 223
Commandes Telnet 223
Exemple 223
4.6 Configuration et connexion d'un réseau sans fil 226
Architecture 227
Fonctionnement d'IEEE 802.11 228
Sécurité du réseau sans fil 229
Présentation d'une carte sans fil 235

5 Les troyens, keyloggers, virus et vers 257

5.1 Méthodes d'introduction d'un cheval de Troie 259
Techniques de camouflage d'un troyen 260
Où se trouve le cheval de Troie ? 264
5.2 Les chevaux de Troie 264
Types de chevaux de Troie 264
5.3 Logiciels troyens et installation détaillée 268
Installation de Back Orifice 268
5.4 Configuration de Senna Spy 2002 273
Fonctionnalités de Perfect Keylogger 1.53 (version démo) 278
5.5 Les virus 282
La détection des virus 282
5.6 Programmes farceurs 284
Simulation de formatage du disque dur 285
Simulation de vidage du système 288
5.7 Les antivirus 289
Le choix de l'antivirus 290
5.8 Troyen ou Administrateur à distance ProRat 291
Créer le serveur 291
Former un serveur 292
Options post connexion 297

6 La force brute 307

6.1 Logiciel de force brute Brutus AET2 309

Détails du programme Brutus 310
Type d'attaque 313
Options d'authentification 315
Mode de craking 315
Création d'un dictionnaire en .txt 317
Brutus en mode d'attaque 318
Capture de Brutus 319
Test de vulnérabilité avec Brutus 320
6.2 Contourner les attaques grâce aux serveurs IIS vs 6.0 Windows 2003 Server 325
Taches nécessaires à effectuer par l'administrateur 326
6.3 Présentation de l0pthcrack 328
Type d'attaque L0pthcrack 329
6.4 Logiciel de force brute Unsecure 349
Attaque options 352
Brute force options 352

7 Les exploits 355

7.1 Le programme Active State 358
7.2 Les exploits perl 360
Fonctions de l'exploit Dnshack 360
Fonctions de l'exploit msacd 366
Fonctions de l'exploit xpu 369
Utiliser xpu.pl 369
Mode d'emploi d'unicodexecute sur MS DOS 370
Fonctions de l'exploit Unicodecheck 371
Fonctions de l'exploit Unicode_shell 372
Fonctions de l'exploit Unicode iix 375
Fonctions de l'exploit dwphp.pl 375
Fonctions de l'exploit pull.pl 376
Fonctions de l'exploit Whisper.pl 377
Fonctions de l'exploit Whois.pl 377
Fonctions de l'exploit VV5.pl 378
Fonctions de l'exploit putdirs-delete.pl 378
7.3 Exploits par logiciels 379
Fonctions de l'exploit Unicode Linux 379
Fonctions de l'exploit Retina 380
Fonctions de l'exploit Nuke 381
Exploit programme d'attaque Nuke it! 382
Exploit Programme d'attaque KiLLmE 383
Exploit Fpipe 383
Exploit Ntis41b 385
Exploit Winfo 387
7.4 Exploit pour trouver des fuites d'information sur Internet 388
Logiciel NET framework 388
Exploit Athena 388
7.5 Exploit Mail bombe 391
Exploit Resource Hacker 392

7.6 Exploit NETCAT pour Windows XP/2000/2003 393
Fonction Scanner de ports 394
Aide de NETCAT pour résoudre une adresse IP d'un ordinateur à distance 395
Ecouter des ports avec NETCAT 397
Fonction sniffer 397
Transfert de fichiers 397
Envoyer des emails Grâce à Netcat 398
7.7 Transfert de zone DNS avec des exploits 399
Transfert de zone grâce à l'exploit DIG pour Windows 402

8 Intrusion, failles système et conséquences 405

8.1 Les bogues d'Unicode 407
Les logiciels d'intrusion 416
Logiciel d'intrusion IISXPLOIT 417
8.2 Logiciel d'intrusion CgiXp ou gl0b4l 420
8.3 Logiciel d'intrusion à distance Unicode Cobra Hack 424
Outil automatisé pour trouver des vulnérabilités 425
Mises en évidence le lecteur C 427
8.4 Logiciel d'intrusion Unicode 428
Retirer des fichiers avec Unicode NT4 de l'ordinateur distant 432
8.5 Le défaçage (ou défiguration) de sites Web 439
Utiliser le logiciel Unicode NT4 440
Ouvrir le contenu du lecteur d'un serveur avec des vulnérabilités 440
8.6 Transfert de données vers l'ordinateur à distance : Upload 442
Défaçages pour les failles d'un Script CGI 446
Contre mesure Unicode 448
8.7 Intrusion dans l'aire wireless pour Windows 448
Logiciel d'intrusion Wireless Air Crack 449
8.8 Logiciel d'intrusion Wireless Airodump 451
Contre mesures pour des attaques aircrack 453
8.9 Manipulation d'enquêtes sur Internet 454
8.10 Capture d'emails 461
8.11 Intrusion sur des Sites de Chat Privés 464

9 Cryptage et décryptage de données 473

9.1 Cryptage de données avec Windows 475
9.2 Cryptages et décryptages de Word 476
Cryptage 477
Décryptage de Word à l'aide d'un programme 478
Programmes de cryptage faibles 480
9.3 Cryptage et décryptage Locktight 480
Cryptage d'un fichier 480
Apercevoir le fichier hola.doc crypté 482
Décryptage de fichiers 482

9.4 Cryptage d'une base de données en Access 483
Décryptage d'une base de données en Access 487
9.5 Le réseau ECHELON 489
9.6 Le PGP 492
Installation de PGP 6.5.1 pour Windows 95/98 492
Envoyer des messages avec PGP 494
Protéger les mots de passe de Microsoft 496
Les hackers et le décryptage des mots de passe Windows 496
Programme d'altération de mot de passe 497
9.7 La stéganographie 499
Présentation de la stéganographie 499
Programme Invisible Secret 500
Application d'Invisible Secret 501

10 Nettoyage et récupération de données 507

10.1 Effacer ses traces manuellement 509
Retirer les programmes 509
Nettoyer la base de registre 510
Les différentes formats des données stockées dans le registre 513
Effacer nos traces des Propriétés d'Internet 514
Effacer les données du journal d'événements 516
Analyser le disque 517
10.2 Effacer ses traces avec des logiciels 518
Steganos destructeur de traces Internet 518
RegCleaner Nettoyeur de traces de la base de registre 519
Super effaceur de traces CuteShield File Shredder 519
L'effaceur multi option EasyCleaner 520
Tambu Registry Editor 521
10.3 Récupération de fichiers 522
Récupération de fichiers dans la base de registre avec le logiciel Undelete 522
Restaurer des données effacées avec Restorer 2000 525
Utiliser Vedit 525
Utiliser Ultraedit Version de démonstration 526
10.4 Récupération d'un mot de passe 527
Revelation 528
Logiciel de destruction de la zone d'amorçage 530
10.5 La façon positive d'utiliser une disquette bombe 533

11 Protégez votre ordinateur 539

11.1 Sauvegarde de données 541
11.2 Le Pare-feu 544
Zone Alarm 546
Configuration du pare-feu de Windows XP 560
Le pare-feu Symantec Norton Internet Security 2006 564
Protection contre les virus 581
Programme de détection de virus NORTON 582

Configuration de Norton antivirus 2005 582
Mises à jour du logiciel 587
Analyse de l'ordinateur 590
Modalité de recherche d'infection sur l'ordinateur 590
Anti-virus Gratuit Scanner en ligne pour désinfecter votre PC 594
11.3 Les Anti-Troyens 604
Détecter la présence d'un cheval de Troie dans votre PC 604
Programme anti-troyen T-ANTI-TROYEN 5.5.420 605
11.4 Les Pots de miel 607
11.5 Les Anti-Sniffer 609
11.6 Anti Tracer 610
11.7 Protection contre les failles du système 611
11.8 Coffre-fort 611
11.9 Logiciels de protection parentale 620
11.10 Protégez-vous avec IPSec 621
11.11 Utiliser Access denied 635
11.12 Protéger les principaux ports de votre ordinateur : Protectx 638
11.13 Retrouver les hackers 639
11.14 Eteindre un ordinateur à distance 641
Logiciel Shutdown 642

12 L'ingénierie sociale 645

12.1 Types d'informations attirantes pour les espions 648
Informations publiques 648
Informations internes 649
Informations privées 649
Informations sensibles 650
12.2 Règles générales d'une attaque d'un espion industriel 650
12.3 Exemple 1 : Manipulation et intrusion à distance 651
Histoire d'une entreprise d'antivirus au bord du dépôt de bilan 651
Élaboration d'un plan 652
Des appels téléphoniques avec une liste de questions clés 652
Dépanner un collègue 655
Réflexion sur la ruse de l'exemple 1 656
12.4 Exemple 2 : Manipulation et entrée physique 658
Un homme calculateur 658
Manipulation psychologique 661
Vol discret 663
Les apparences trompeuses 663
Réflexion sur la ruse 2 664
12.5 Exemple 3 : Manipulation et intrusion avec un complice 665
Harcèlement d'une personne 666
Altération d'une page web 667
Manipulation avec un alibi 667
Aider un collègue en difficulté 668
Résultat de la ruse de l'exemple 3 668

12.6 Exemple 4 : Intimidation et déséquilibre émotionnel 669
Vengeance d'un ex salarié 669
Interception illicite 670
Vente d'un produit à la concurrence 671
Complice à volonté 673
Déstabilisation émotionnelle 673
Intimidation 674
Recommandation 676
Nous sommes là pour vous aider 677
Fausse panne 678
Monsieur manipulateur, j'ai besoin de vous 679
La victime vous fait totalement confiance 679
Réflexion sur la ruse de l'exemple 4 681
12.7 Exemple 5 : Usurpation de l'identité physique et stratégie de la compassion 682
Poubelle 682
Usurpation physique d'identité 683
Accident intentionnel 683
Entrée dans un endroit sécurisé par la grande porte 684
Stratégie de la compassion 684
Réflexion sur la ruse de l'exemple 5 686
12.8 Exemple 6 : Fusion 687
Plan d'action 688
La fusion des entreprises 688
Personnel avec des papiers falsifiés 690
Les futures occupations de l'espion une fois en poste 690

13 Le phishing et vulnérabilités des pages Web 693

13.1 La technique du phishing 695
Protégez-vous contre les attaques du phishing 695
Antiphishing 696
Objectifs du phishing 697
13.2 Exemple 1 : Les banques en danger 697
Séduction 698
Détournement d'appel 700
Connexion Internet dans une maison vide 701
Restauration de la vraie page par l'intermédiaire d'un complice à l'étranger 702
Recommandations 702
Réflexion sur la ruse de l'exemple 1 703
13.3 Exemple 2 : Simulation d'attaque avec phishing 704
XSS (Cross Site Scripting) dans des serveurs sécurisés 704
Explication du phishing 707
Démonstration d'un cas réel de phishing 711
Recommandations 715
Éviter d'être pris au piège par le phishing 717
13.4 Altération d'une page web 719
Les scripts malveillants 720

14 La sécurité des entreprises 723

14.1 Tactiques d'attaques courantes 725
Tactiques d'une attaque à distance 726
Tactiques d'une attaque en utilisant la manipulation 726
14.2 Protéger votre entreprise 727
14.3 Protection des informations publiques 728
Achats en ligne 728
Ligne téléphonique 730
Annonces publicitaires 730
Personnel recevant des appels 730
Spams à volonté 730
Protection de la boîte vocale 730
Procédures pour des envois des colis 730
14.4 Protection des informations internes et implémentation de matériel 731
Création de badges de couleurs différentes 731
Ligne téléphoniques avec différentes sonneries 731
Traçage d'appel 731
Annuaire 732
Création des stratégies de mot de passe fort 732
Installation des antivirus, anti-troyen, pare-feu 732
Caméras de surveillance 732
Stratégie pour ne pas voir les propriétés du système 733
Stratégie pour désactiver les outils amovibles 733
Couleur et sensibilité des informations 733
Photocopieuse 733
Configuration fax, routeur 733
Mise en place de système biométrique dans des endroits sensibles 734
Destruction d'informations sensibles ou de matériel contenant des informations sensibles 735
Configuration du modem 735
Protection des poubelles 735
Informations internes 736
Configuration des réseau sans fil 736
Configuration du moniteur réseau 737
Installation de pare-feu interne et externe 737
Privilèges des utilisateurs 737
Formation des employés 737
Création d'un groupe de gestion des incidents 738
Formation des salariés 738
Catégories des informations 739
Responsables hiérarchiques 739
Diffusion d'informations à un tiers 740
Éviter la manipulation téléphonique 741
14.5 Informations sensibles 742
Test de vulnérabilité 743
14.6 Vérification des antécédents 747

14.7 Recommandations aux administrateurs réseau 747
14.8 Recommandations aux utilisateurs 749
14.9 Sécuriser votre entreprise contre les vulnérabilités wireless 750
14.10 Test de vulnérabilité Scan Modem et RAS (Remote Access Server) 755
14.11 Vulnérabilité du pare-feu et protection de NAT 757

15 Annexe 1 – Glossaire 761

16 Annexe 2 - Les logiciels 779

16.1 Scanners 783
Super scan3 783
Nettols 783
Stealth 783
Urlscanner 783
Toneloc 784
Scanner de page web : Acunetix 784
N-Stealth HTTP Security Scanner 784
Logiciel ProxyHunter 784
16.2 Traceurs 785
Visualroute 785
Neotrace 785
16.3 Renifleurs 785
Logiciel sniffer Ettercap 785
Logiciel sniffer Ethereal 785
Mpsnif 785
Logiciel X-NetStat Professional 786
16.4 Renifleurs sans fil 786
Cain & Abel 786
Airopeek 786
Netstumbler 786
16.5 Crack de mot de passe 786
l0Phcrack 787
Logiciel Air Crack pour Windows 787
16.6 Internet anonyme 787
Stealth_Anonymizer_27 787
Steganos Internet Anonyme 787
16.7 Antimouchards 787
Ad-adware 788
Spybot-Search & Destroy 788
Cookie pal 788
XP-Antispy 788
16.8 Troyens 788
Back Orifice 788
Senna 2002 789
Logiciel Netbus 2.20 789

16.9 Force brute 789
Brutus 789
16.10 Analyseurs de failles 789
Active State 789
Cgis4 790
Retina 790
Dsnhack 790
Lishack 790
Msacd 790
Unicodecheck 790
Unicode IIS 790
KILLmE 791
Fpipe 791
Exploit ntis41b 791
Exploit Winfo 791
Exploit Resource Hacker 791
16.11 Cryptage et décryptage 791
MS WORD 791
Locktight 792
Winrar 792
Hackman 792
PGP 792
16.12 Stéganographie 792
Invisible secret 792
16.13 Destructeur de traces 793
Steganos Destructor 793
Regclearner 793
Cuteshield 793
Tamburegistry 793
16.14 Récupérateurs de données 793
Undelete 793
Restorer 2000 794
Vedit 794
Revelation 794
16.15 Anti-troyens 794
Anti-troyen 794
Netbuster 794
16.16 Anti-tout 794
Symantec Norton Anti-Virus 795
Antisniffer 795
Antitracer 795
Antiphishing 795
16.17 Détection d'intrusion 795
Acces Denied 795
Coffre-fort 795
16.18 Les pare feu 796
ZoneAlarm 796
Pare feu Windows 796
Le pare feu Sygate 796

16.19 Autres outils utiles **796**
Virtual Machine 796
Keylogger 796

17 **Annexe 3 - Architecture et fonctionnement de TCP/IP** **797**

17.1 Architecture du protocole **799**
Couche Interface réseau 800
Couche Internet 801
Couche Transport 801
Couche Application 802
17.2 Protocoles centraux TCP/IP **803**
IP 804
Segmentation et réassemblage 804
ARP 805
ICMP 806
IGMP 807
TCP 809
UDP 810
17.3 Interfaces d'application de TCP/IP **812**
17.4 Adressage IP **812**
17.5 Classes d'adresses **813**
Les adresses de classe A 814
Les adresses de classe B 814
Les adresses de classe C 814
Les adresses de classe D 814
Les a dresses de classe E 814
17.6 Sous-réseaux et nombre d'hôtes **815**
17.7 L'INTERNIC (www.internic.net) the Internet's Network Information **815**

18 **Annexe 4 - Lois contre le piratage** **817**

18.1 Lois sur la protection intellectuelle (CNIL) **819**
18.2 Articles du code pénal sur le piratage en France **820**
Article 323-1 820
Article 323-2 820
Article 323-3 821
Article 323-4 821
Article 323-5 821
Article 323-6 822
Article 323-7 822

19 **Index** **823**